REPORT DOCUMENTATION PAGE

AFRL-SR-BL-TR-01-

0088

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE

3. REPORT TYPE AND DATES COVERED
01 May 1997 - 31 Dec 1998

4. TITLE AND SUBTITLE
Turbo Decoding of High performance Error-Correcting Codes via Belief Propagation

5. FUNDING NUMBERS
F49620-97-1-0313

6. AUTHOR(S)
Robert McEliece

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Departrment of Electrical Engineering
MS 136-93
California Institute of Technology
Pasadena, CA 91125

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR
801 North Randolph Street, Room 732
Arlington, VA 22203-1977

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
F49620-97-1-0313

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release. Distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

We studied AWGN coding theorems for ensembles of coding systems which are built from fixed convolutional codes interconnected with random interleavers. We call these systems turbo-like codes and they include as special cases both the classical turbo codes and the serial concatenation of interleaved convolutional codes. We offered a general conjecture about the behavior of the ensemble (maximum-likehood decoder) word error probability as the word length approaches infinity. We proved this conjecture for a simple class of rate 1/q serially concatenated codes where the outer code is a q-fold repetition code and th inner code is rate 1 convolutional code with transfer function $1/(1+D)$. We call these codes "RA" (repeat and accumulate) codes. This was the first rigorous proof of a coding theorem for turbo-like codes.

20010220 013

14. SUBJECT TERMS

15. NUMBER OF PAGES
1

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

NM

FINAL TECHNICAL REPORT on AFOSR grant no. F49620-97-0313:

"Turbo Decoding of High performance Error-Correcting Codes via Belief Propagation"

PRINCIPAL INVESTIGATORS:

Robert J. McEliece
Department of Electrical Engineering
MS 136-93
California Institute of Technology
Pasadena, CA 91125

Padhraic Smyth
Department of Information and Computer Science
University of California
Irvine, CA

OBJECTIVES: No change from those stated in the original proposal.

STATUS OF EFFORT: The work went extremely well at both institutions. We had frequent joint meetings (approx. 1 per month) in which each group informed the other about its progress. Technical details follow.

ACCOMPLISHMENTS/NEW FINDINGS:

***At Caltech:

We studied AWGN coding theorems for ensembles of coding systems which are built from fixed convolutional codes interconnected with random interleavers. We call these systems ``turbo-like" codes and they include as special cases both the classical turbo codes and the serial concatenation of interleaved convolutional codes. We offered a general conjecture about the behavior of the ensemble (maximum-likelihood decoder) word error probability as the word length approaches infinity. We proved this conjecture for a simple class of rate 1/q serially concatenated codes where the outer code is a q-fold repetition code and the inner code is a rate 1 convolutional code with transfer function 1/(1+D). We call these codes "RA" (repeat and accumulate) codes. This was the first rigorous proof of a coding theorem for turbo-like codes.

These results show that the performance of RA codes with maximum-likelihood decoding is very good. However, the complexity of ML decoding of RA codes, like that of all turbo-like codes, is prohibitively large. But an important feature of turbo-like codes is the availability of a simple iterative, message passing decoding algorithm that approximates ML decoding. We wrote a computer program to implement this "turbo-like" decoding for RA codes with q=3 (rate 1/3) and q=4 (rate 1/4), and the results were remarkably good. For example, with an information block length of 16384, the q=4 RA code achieves a decoded word error probability of about 10^{-5} at E_b/N_0 = 0.5 dB with 20 decoding iterations.

This work demonstrated that there is a much less complex way to achieve near Shannon limit performance than was previously suspected.